Flux, flux и в production

Медведев Виталий





С чем мы живём

2003

Solaris

5 серверов

20 сервисов

Ручной деплой



Процессы

Установка – вручную, всякий раз по новому

Артефакты - любые

Длительность непредсказуема (2 недели – это быстро)

В процессе задействованы минимум 3 отдела

Все изменения на production через эксплуатацию



С чем мы живём

2003

Solaris

5 серверов

20 сервисов

Ручной деплой

2014

Linux

20 HV/300+ VM

100 сервисов

Puppet



Процессы

Установка - puppet/утилиты (95/5)

Артефакты – rpm и рецепты puppet

Длительность – до 30 минут (1 час это уже долго)

В процессе задействованы минимум 2 отдела

95% изменений на production через эксплуатацию



С чем мы живём

2003	2014	2018
Solaris	Linux	Kubernetes
5 серверов	20 HV/300+ VM	3 кластера/70 нод
20 сервисов	100 сервисов	300 сервисов
Ручной деплой	Puppet	Fluxcd



Процессы (планы)

Установка – helm upgrade

Артефакты – chart

Длительность – до 15 минут

В процессе задействованы минимум 2 отдела

Изменения на production через эксплуатацию



Ожидания

Сделать всё хорошо

Делается всё хорошо



Реальность



Горшочек, не вари

Вырос штат => ops/dev = 1/30



Горшочек, не вари

Вырос штат => ops/dev = 1/30

Количество версий в неделю увеличилось на порядок



Горшочек, не вари

Вырос штат => ops/dev = 1/30

Количество версий в неделю увеличилось на порядок

Нет автоматизации => ошибки при ручной установке



заделпой пару чартов

и нам заделпой

што праисходет?

ДЕПЛООООЙ!!!

памагити

Горшочек, не вари

Вырос штат => ops/dev = 1/30

Количество версий в неделю увеличилось на порядок

Нет автоматизации => ошибки при ручной установке

Изменения в инфраструктуре, которые нигде не фиксировались



заделпой пару чартов

и нам заделпой

што праисходет?

ДЕПЛООООЙ!!!

памагити

Горшочек, не вари

- Вырос штат => ops/dev = 1/30
- Количество версий в неделю увеличилось на порядок
- Нет автоматизации => ошибки при ручной установке
- Изменения в инфраструктуре, которые нигде не фиксировались
- Бесконечный helm upgrade



Нормально делай – нормально будет

Infrastructure-as-code



Нормально делай – нормально будет

Infrastructure-as-code

История и аудит изменений



Нормально делай – нормально будет

Infrastructure-as-code

История и аудит изменений

Соответствие требованиям ИБ



Нормально делай – нормально будет

Infrastructure-as-code

История и аудит изменений

Соответствие требованиям ИБ

Одинаковая процедура развёртывания



Нормально делай – нормально будет

Infrastructure-as-code

История и аудит изменений

Соответствие требованиям ИБ

Одинаковая процедура развёртывания

Эволюция, а не революция



GitOps – хайп или решение?





Git – source of truth

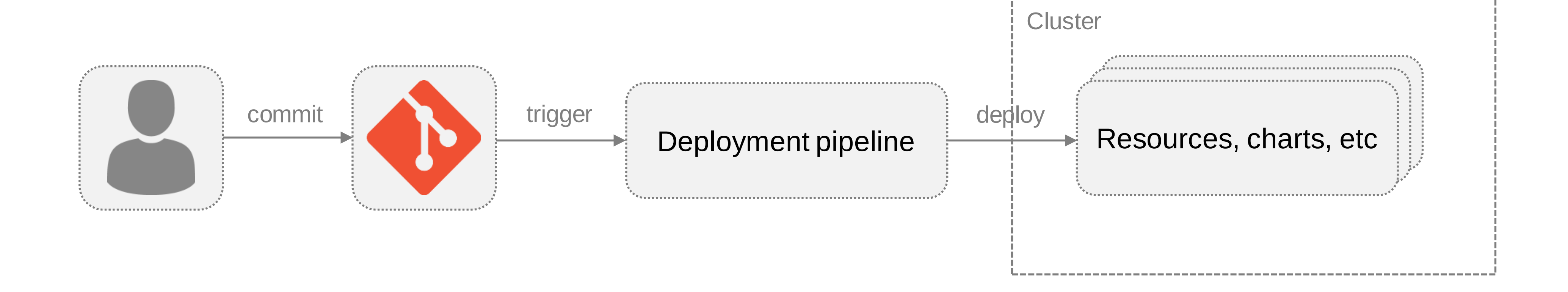
Изменения в кластере только через изменения в репозитории

Нет разницы в процедуре деплоя между окружениями

Pull или push?



Push?

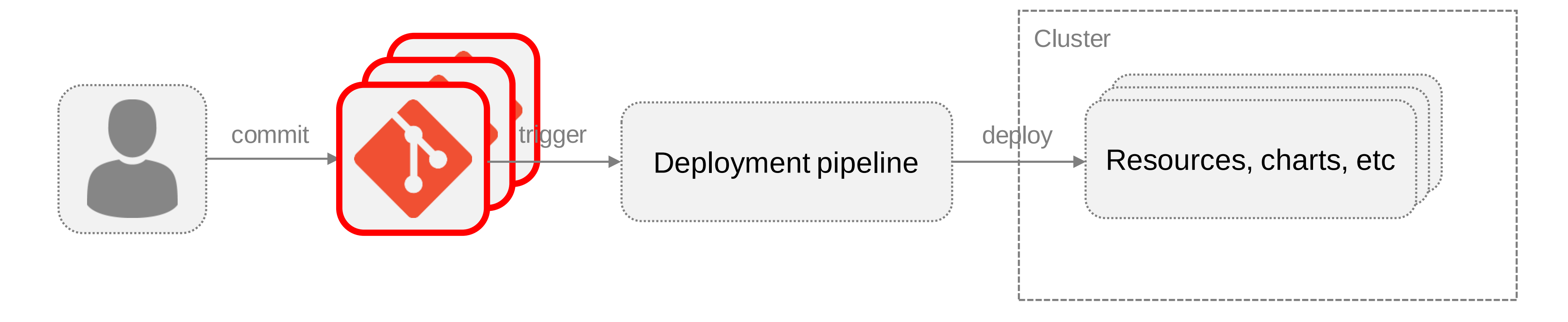


commit
trigger
Deployment pipeline
Cluster
deploy
Resources, charts, etc



HL
HighLoad++
Весна 2021

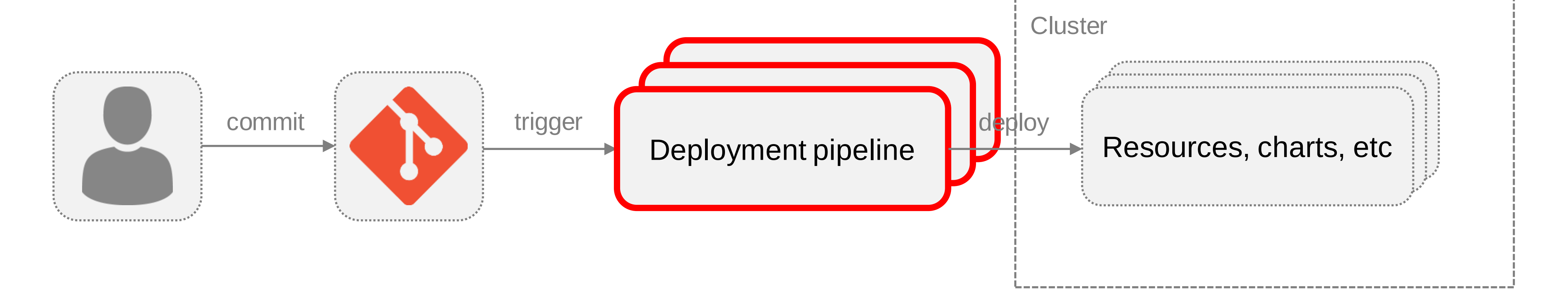
Push?



Разные системы управления репозиториями



Push?

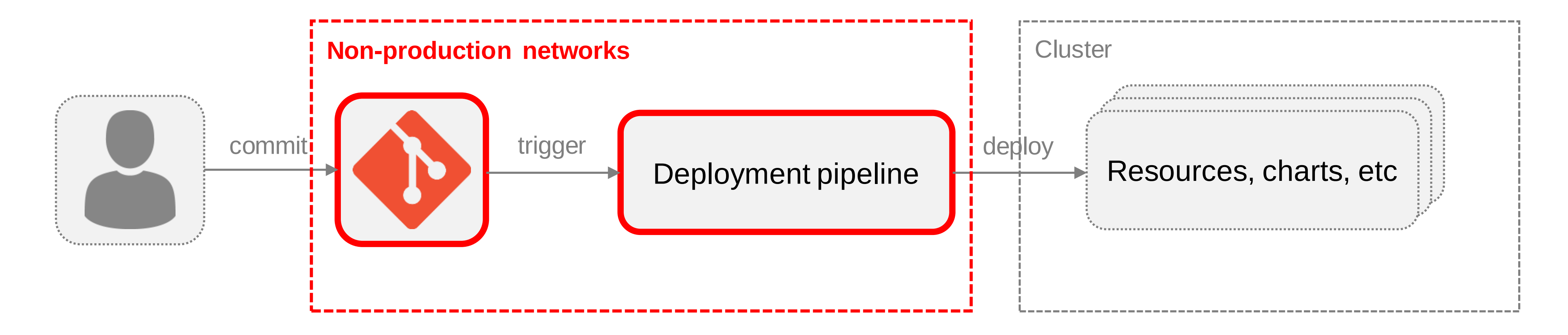


Разные системы управления репозиториями

Разные инструменты CI/CD



Push?



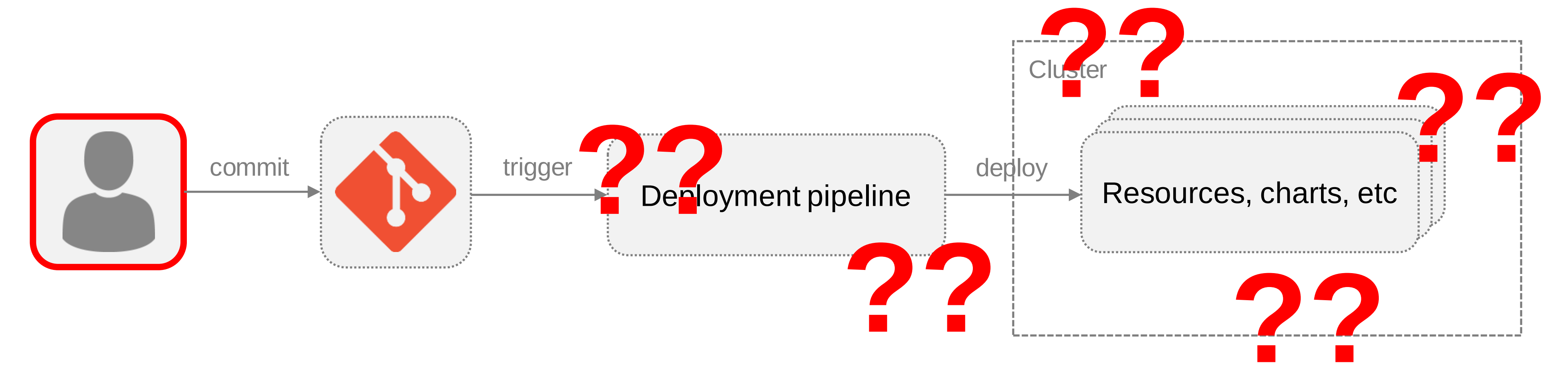
Разные системы управления репозиториями

Разные инструменты CI/CD

Трудно соблюдать требования ИБ и регулятора



Push?



Разные системы управления репозиториями

Разные инструменты CI/CD

Трудно соблюдать требования ИБ и регулятора

Разный уровень компетенции в командах



Push?



Разные системы управления репозиториями

Разные инструменты CI/CD

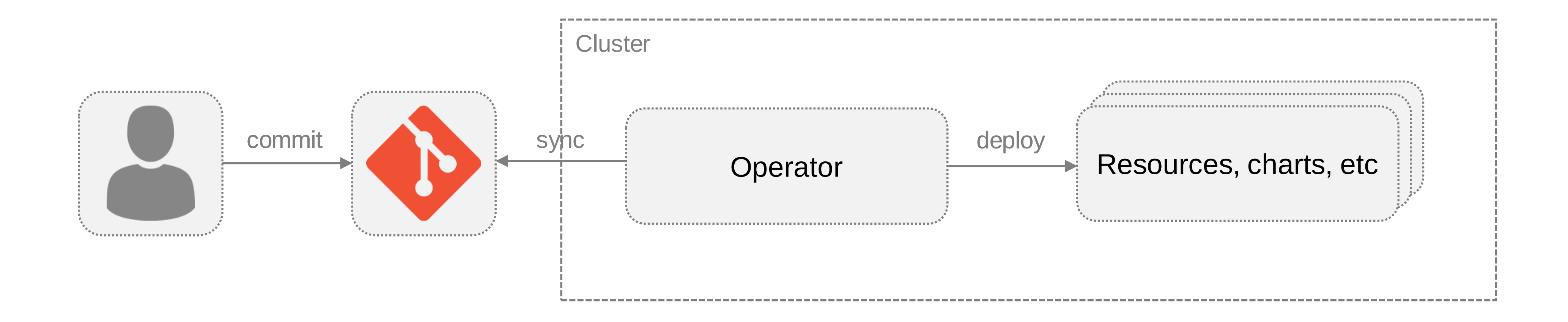
Трудно соблюдать требования ИБ и регулятора

Разный уровень компетенции в командах

Количество команд и отношение ops/dev = 1/30



Pull!

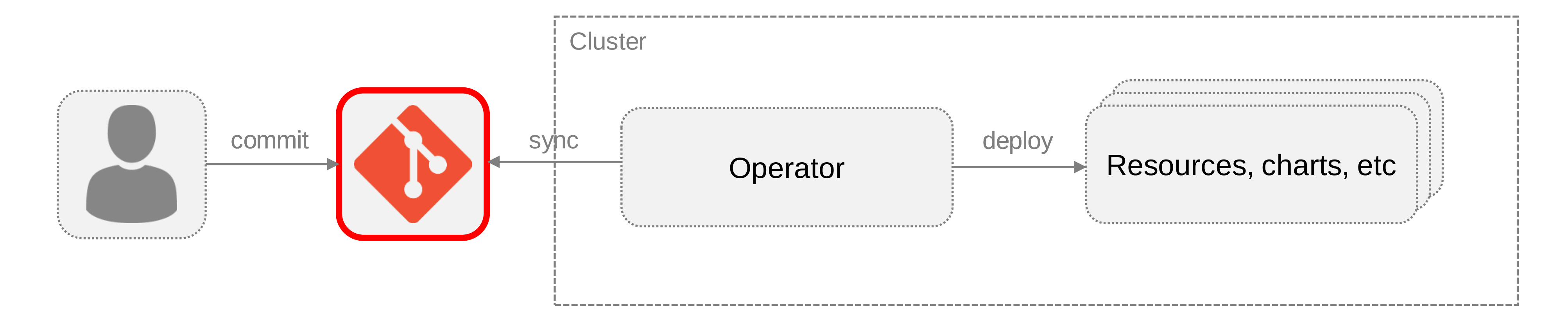


commit
sync
Cluster
Operator
deploy
Resources, charts, etc



HL
HighLoad++
Весна 2021

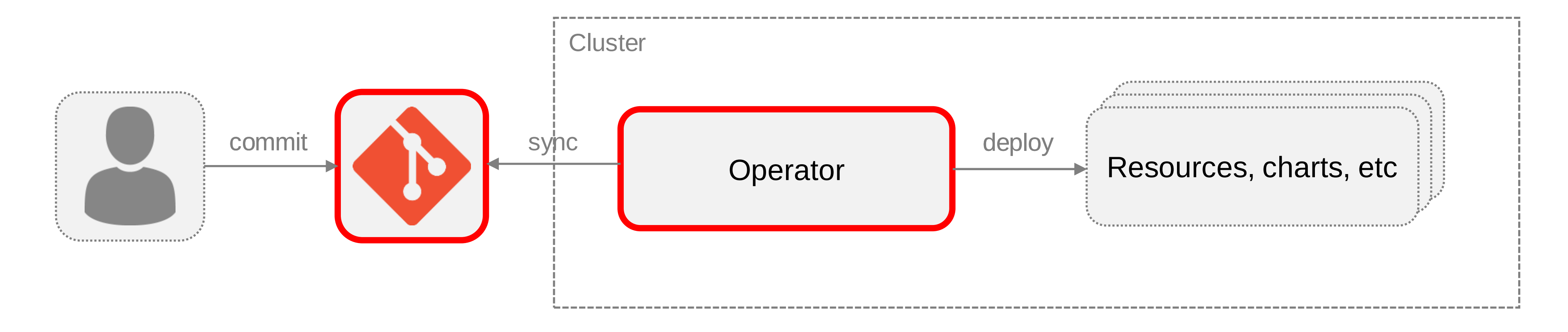
Pull!



Единая система управления репозиториями



Pull!

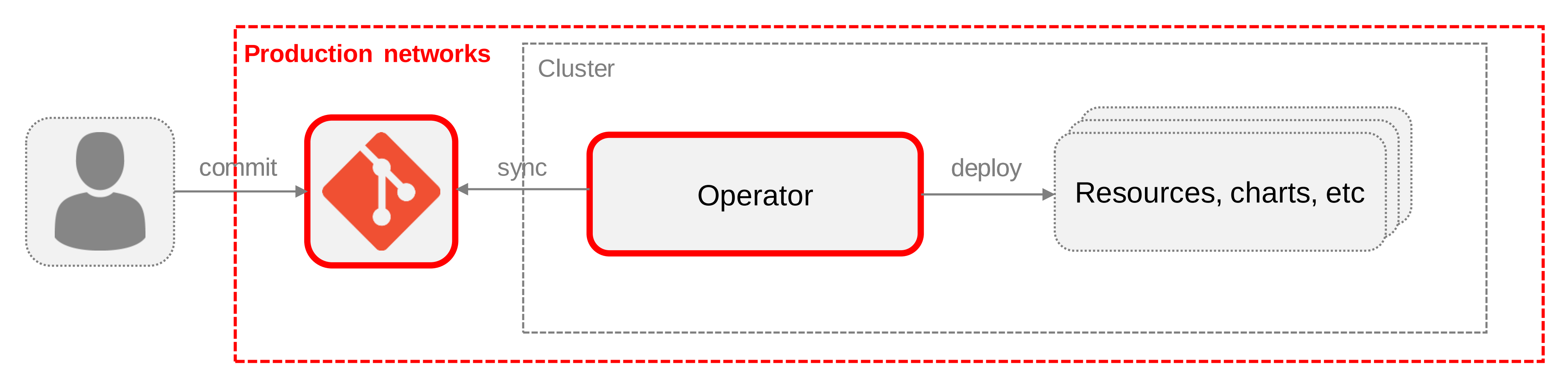


Единая система управления репозиториями

Доступ на основе RBAC



Pull!



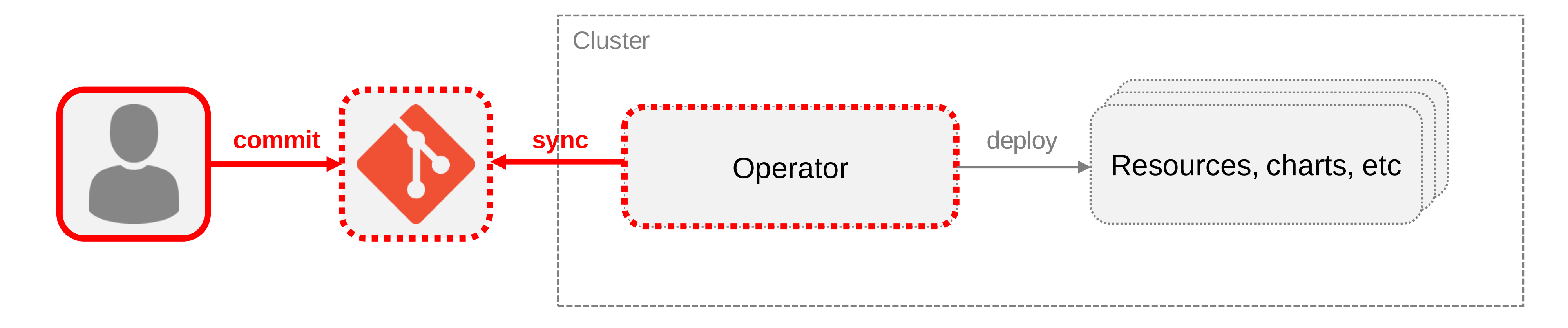
Единая система управления репозиториями

Доступ на основе RBAC

Контролируется эксплуатацией, благословлено ИБ



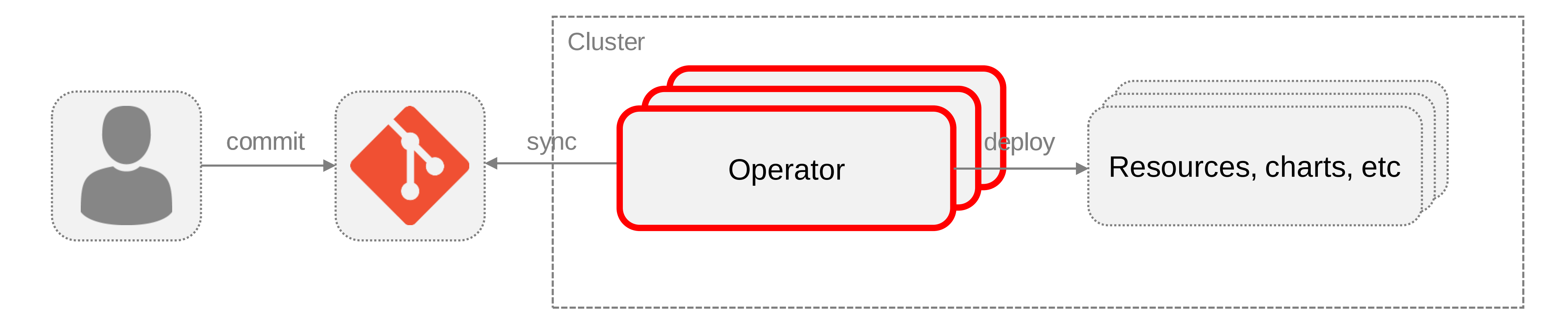
Pull!



Единая система управления репозиториями
Доступ на основе RBAC
Контролируется эксплуатацией, благословлено ИБ
Базовые знания и простые инструменты



Pull!



Единая система управления репозиториями
Доступ на основе RBAC
Контролируется эксплуатацией, благословлено ИБ
Базовые знания и простые инструменты
Легко масштабировать



Cluster admin

commit

Git repository

sync

Cluster

Flux
system

apply

Cluster
resources

apply

HelmRelease
resources

Helm operator
system

watch

install/upgrade/delete

HELM

Charts
system

Namespace

Team member

commit

Git repository

sync

Flux
namespace

apply

Namespace
resources

apply

HelmRelease
resources

Helm operator
namespace

watch

install/upgrade/delete

HELM

Charts
namespace



Cluster admin

Cluster

apply

Cluster resources

install/upgrade/delete

Charts
system

Namespace

apply

Namespace resources

install/upgrade/delete

Charts
namespace



Cluster admin

Cluster

install/upgrade/delete

Prometheus operator

system

Namespace monitoring

Prometheus resources



Cluster admin

Cluster

install/upgrade/delete

Prometheus operator
system

Namespace monitoring

Git repository

apply

Prometheus resources

commit

sync

Flux
namespace



Cluster admin

Cluster

Namespace

Team member

Git repository

commit

sync

apply

Flux
namespace

Namespace resources



Cluster admin

Team member

Git repository

commit

sync

Cluster

Namespace

Flux
namespace

apply

Namespace resources



Cluster admin

Cluster

Namespace

Team member

Git repository

commit

sync

apply

Flux
namespace

Namespace resources



Cluster admin

Git repository

commit

sync

Cluster

apply

Flux
system

Cluster
resources

Namespace

Team member

Git repository

commit

sync

apply

Flux
namespace

Namespace
resources



Cluster admin

Git repository

commit

sync

Cluster

Flux
system

apply

Cluster
resources

install/upgrade/delete

Charts
system

Namespace

Team member

Git repository

commit

sync

Flux
namespace

apply

Namespace
resources

install/upgrade/delete

Charts
namespace



Cluster admin

commit

Git repository

sync

Cluster

Flux
system

apply

Cluster resources

install/upgrade/delete

HELM

Charts
system

Namespace

Team member

commit

Git repository

sync

Flux
namespace

apply

Namespace resources

install/upgrade/delete

HELM

Charts
namespace



Cluster admin

Git repository

commit

sync

Cluster

apply

Flux
system

Cluster
resources

Team member

Git repository

commit

sync

Namespace monitoring

apply

Flux
namespace

Namespace
resources

apply

HelmRelease
resources

Helm operator
namespace

watch

install/upgrade/delete

Charts
namespace



Cluster admin

Git repository

commit

sync

Cluster

apply

Flux
system

Cluster
resources

Namespace

Team member

Git repository

commit

sync

apply

Flux
namespace

Namespace
resources

apply

HelmRelease
resources

Helm operator
namespace

watch

install/upgrade/delete

HELM

Charts
namespace



Cluster admin

commit

Git repository

sync

Cluster

apply

Flux
system

Cluster resources

Team member

commit

Git repository

sync

Namespace

apply

Flux
namespace

Namespace resources

apply

HelmRelease resources

Helm operator
namespace

watch

install/upgrade/delete

Charts
namespace



Cluster admin

Git repository

commit

sync

Cluster

apply

Flux
system

Cluster resources

Team member

Git repository

commit

sync

Namespace

apply

Flux
namespace

Namespace resources

apply

HelmRelease resources

Helm operator
namespace

watch

install/upgrade/delete

Charts
namespace



Cluster admin

Git repository

commit

sync

Cluster

apply

Flux
system

Cluster
resources

Team member

Git repository

commit

sync

Namespace

apply

Flux
namespace

Namespace
resources

apply

HelmRelease
resources

Helm operator
namespace

watch

install/upgrade/delete

HELM

Charts
namespace



Cluster admin

Git repository

commit

sync

Cluster

Flux
system

apply

Cluster resources

apply

HelmRelease resources

Helm operator
system

watch

install/upgrade/delete

HELM

Charts
system

Namespace

Team member

Git repository

commit

sync

Flux
namespace

apply

Namespace resources

apply

HelmRelease resources

Helm operator
namespace

watch

install/upgrade/delete

HELM

Charts
namespace



Cluster admin

commit

Git repository

sync

Cluster

Flux
system

apply

Cluster resources

apply

HelmRelease resources

Helm operator
system

watch

install/upgrade/delete

Charts
system

Namespace

Team member

commit

Git repository

sync

Flux
namespace

apply

Namespace resources

apply

HelmRelease resources

Helm operator
namespace

watch

install/upgrade/delete

Charts
namespace



Cluster admin

commit

Git repository

sync

Cluster

Flux
system

apply

Cluster resources

apply

HelmRelease resources

Helm operator
system

watch

install/upgrade/delete

Charts
system

Team member

commit

Git repository

sync

Namespace

Flux
namespace

apply

Namespace resources

apply

HelmRelease resources

Helm operator
namespace

watch

install/upgrade/delete

Charts
namespace



Структура репозитория

```
├── production
│   └── helm-releases
│       └── production-release.yaml
└── test
    └── helm-releases
        ├── test-release1.yaml
        └── test-release2.yaml
```




Структура репозитория

```
├── production
│   └── helm-releases
│       └── production-release.yaml
└── test
    └── helm-releases
        ├── test-release1.yaml
        └── test-release2.yaml
```

```yaml
apiVersion: helm.fluxcd.io/v1
kind: HelmRelease
metadata:
  name: helm-release-name
spec:
  releaseName: helm-release-name
  chart:
    repository: git@git:project/chartrepo.git
    ref: 2.0.0-560
    path: .
```




Структура репозитория

```
├── production
│   └── helm-releases
│       └── production-release.yaml
└── test
    └── helm-releases
        ├── test-release1.yaml
        └── test-release2.yaml
```

```yaml
apiVersion: helm.fluxcd.io/v1
kind: HelmRelease
metadata:
  name: helm-release-name
spec:
  releaseName: helm-release-name
  chart:
    repository: git@git:project/chartrepo.git
    ref: 2.0.0-560
    path: .
```




Структура репозитория

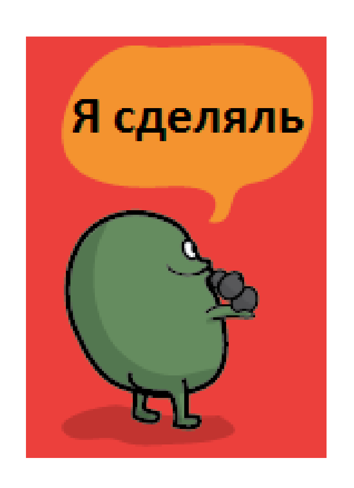
```
├── production
│   └── helm-releases
│       └── production-release.yaml
└── test
    └── helm-releases
        ├── test-release1.yaml
        └── test-release2.yaml
```

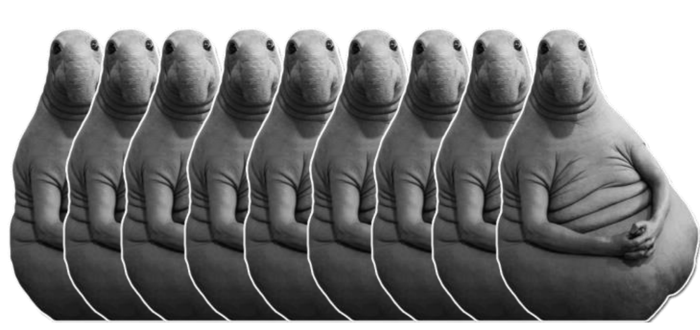
```yaml
apiVersion: helm.fluxcd.io/v1
kind: HelmRelease
metadata:
  name: helm-release-name
spec:
  releaseName: helm-release-name
  chart:
    repository: git@git:project/chartrepo.git
    ref: 2.0.0-560
    path: .
```

```yaml
apiVersion: helm.fluxcd.io/v1
kind: HelmRelease
metadata:
  name: helm-release-name
spec:
  releaseName: helm-release-name
  chart:
    repository: git@git:project/chartrepo.git
    ref: master
    path: .
  valuesFrom
    - chartFileRef:
        path: 'values/env.yaml'
```



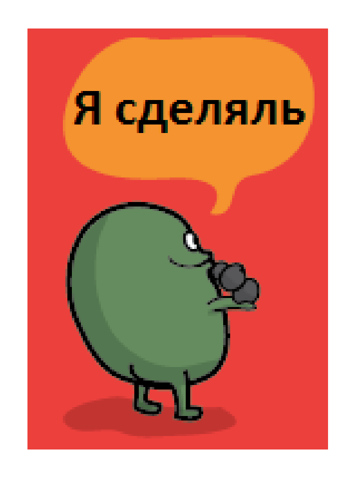

Результаты













Время на деплой уменьшилось в 60 раз

Нагрузка на инженеров в 10 раз

Ни один релиз не пострадал

IaC для инфраструктуры

CD там, где его никогда не было



Процессы

Установка – merge => helm upgrade

Артефакты – chart и helmRelease

Длительность – до 15 минут

В процессе задействованы минимум 1 отдел

Изменения на production через эксплуатацию, сопровождение, разработку



Ложка дёгтя

Observability процессов CD



Ложка дёгтя

Observability процессов CD

Разные репозитории для кода/чартов/конфигурации



Ложка дёгтя

Observability процессов CD

Разные репозитории для кода/чартов/конфигурации

Комплексные чарты с зависимостями



Выводы

Gitops – проще, чем кажется



Выводы

Gitops – проще, чем кажется

Развивайте то, что уже существует



Выводы

Gitops – проще, чем кажется

Развивайте то, что уже существует

Серебряной пули не существует



Спасибо за внимание

Flux, flux и в production

Виталий Медведев

v.medvedev@cft.ru

